REMARKS

Reconsideration of the application is requested.

Claims 1-17 remain in the application. Claims 1-17 are subject to examination. Claims 1, 2, 6-9, and 11-17 have been amended.

Under the heading "Specification" on page 2 of the above-identified Office Action, the Examiner objected to the disclosure because of a number of informalities.

Applicant appreciates the indication of the numerous informalities that were caused by a poor translation. Numerous amendments to the specification have been presented to correct the errors in the specification. The material in the portions of the specification appearing on pages 4, 5, 6, and 8 of the previous amendment has been changed to read, " In accordance with an object of the invention, there is provided ...". The errors in portions of the specification appearing on pages 9, 12, 15, 16, and 18 of the previous amendment have been addressed. As the Examiner requested, great effort has been expended in examining the entire application to identify and correct all possible minor errors and to present the subject matter in a more readable format. Applicant expresses gratitude for the effort of the Examiner in working to correct these informalities.

Under the heading "Claim Objections" on page 4 of the above-identified Office Action, the Examiner objected to claims 1, 11, 13-15, and 17 because of two (2) informalities.

Applicant appreciates the indication of the informalities and the Examiner's suggested corrections have been made.

The term "supply power" has been changed to "power" throughout the claims. In claim 14, a comma has been inserted after controlling/

Under the heading "Claim Rejections – 35 USC § 112" on page 5 of the above-identified Office Action, claims 6, 7, 9, and 11-17 have been rejected as being indefinite under 35 U.S.C. § 112, first / second paragraph.

With regard to claim 6, the Markush group has been properly defined, the terms "irregularity" and "additional operating parameters" have been deleted from the claim. It is believed that the phrase "fluctuation of the supply voltage" is clear.

The American Heritage Dictionary of the English Language: Fourth Edition (2000) defines fluctuation as follows: 1. To vary irregularly. 2. To rise and fall in or as if in waves; undulate.

With regard to claim 7, the Markush group has been properly defined, and the terms "as well as" have been changed to "and".

With regard to claim 9, the narrative phrase has been rewritten and the term "previously received version" has been deleted.

With regard to claim 11, "supply power" has been changed to "power" and antecedent basis for power is found within the claim.

With regard to claim 13, the objectionable limitation has been rewritten to specify that for each communication operation between the terminal and the security module, the data interface controlled to: send at least the part of the algorithm code or the complete algorithm code to the volatile memory of the security module and then to receive the algorithm code result from the security module. Support for the change is believed to be inherent in the claim.

With regard to claim 14, the preamble has been amended to read:
A process for controlling a security module using a terminal in order to obtain an algorithm code result from the security module, the process comprising performing the following steps during each one of a plurality of communication operations between the terminal and the security module. Support for the change is believed to be inherent in the claim.

With regard to claim 15, the objectionable limitation has been rewritten to specify that the power is being supplied from the terminal. Support for the change is believed to be inherent in the claim.

With regard to claim 17, the objectionable limitation has been rewritten to define a non-volatile memory in which a remainder of the algorithm code which, along with the received part of the algorithm code, forms a complete algorithm code, is stored. . Support for the change is believed to be inherent in the claim.

The following additional clarifying amendments have also been made:

Claim 2 has been amended to more clearly specify the intended limitation. Support for the change is believed to be inherent in the claim.

Claim 8 has been amended to use the terms " consisting of one or more of".

Claim 16 has been amended to delete a second consecutive occurrence of the word "the".

Claim 17 has been amended to us the terms "part" and "remainder" instead of first part and second part.

It is accordingly believed that the specification and the claims meet the requirements of 35 U.S.C. § 112, second paragraph. The above-noted changes to the claims are provided solely for clarification or cosmetic reasons. The changes are neither provided for overcoming the prior art nor do they

narrow the scope of the claim for any reason related to the statutory requirements for a patent.

Under the heading "Claim Rejections – 35 USC § 103" on page 7 of the above-identified Office Action, claims 1-17 have been rejected as being obvious over U.S. Patent No. 4,777,355 to Takahirain view of U.S. Patent No. 5,768,382 to Schneier et al. under 35 U.S.C. § 103. Applicant respectfully traverses.

Schneier et al. are concerned with game cartridges, and distributing and safely collecting computer game outcomes. In connection with these game cartridges, Schneier et al. suggests using the inherent deletion property of volatile memories in order to protect susceptible data, such as, parts of the computer game against tampering by unauthorized persons. Thus, in the normal operation and the normal lifetime, Schneier's game cartridges are intended to have the susceptible data stored in the volatile memory. Only in the case of tampering, will the resulting interruption of power cause the susceptible data to be erased (compare the second paragraph of column 14). To be even more precise, no portion of Schneier et al. teaches or suggests storing the susceptible data in a volatile memory of an object again and again within terminal sessions in order to prevent the susceptible data from being susceptible to attacks of third parties in the meantime. Accordingly, Schneier et al. require that a power source 27 be present in the game cartridge in order to continuously provide power to the volatile memory during the non-tamper times.

In contrast, independent claims 1, 11, 13, 14, 15, and 17 of the present application also include the following limitation: "... such that said volatile memory will be cleared upon an interruption of the receipt of the power from the terminal".

Therefore, Schneier's et al. disclosure could not motivate one of ordinary skill in the art to modify the teaching of Takahira in such a way that the claimed subject matter is obtained.

Looking at the situation differently, Schneier et al. teach storing susceptible data in a volatile memory merely as a well-known measure for securing computer memory devices, i.e. as a well-known alternative to actively deleting stored data from a non-volatile memory (compare the first paragraph in column 14). Again, the inherent deletion of data stored in a volatile memory upon the interruption of power to the volatile memory is merely used to execute the exceptional deletion in case of a tampering. In contrast thereto, it is the intention of the present application to have the data stored in the volatile memory merely during terminal sessions where power is supplied to the volatile memory. Therefore, while in Schneier et al. the storage of the susceptible data into the volatile memory takes place just once within the secure environment of the game program supplier, storing the data into the volatile memory in accordance with the present invention takes place in each terminal session or

communication operation between the terminal and the security module (see claim 13 of the present application).

Takahira in turn, by chance (see "CMOS-RAM" in column 6, line 37) mentions downloading data in to a volatile memory of an IC card merely in connection with test programs for testing the IC cards before their issuance. Accordingly, Takahira does also not suggest protecting an algorithm code concerning the processing of secrets of a security module by storing the algorithm code within a volatile memory of the security module so that this algorithm code is not susceptible to attackers during non-terminal session times.

Further, applicant questions what motivation would exist for one of ordinary skill in the art to combine the teachings of Takahira and Schneier et al. in view of the above considerations. Why would one of ordinary skill in the art provide an IC card with a power supply on it, even though an IC card is already protected by being integrated into a chip and even though the IC card does not have a cartridge housing functioning such that when the housing is opened because of a tampering event, it triggers the disconnection from the power in case of Schneier et al.?

Even if for some reason, one of ordinary skill in the art were motivated by Schneier et al. to build a module having a power supply on it as well as a tamper switch that causes an interruption in the power between the power supply and the volatile memory in the case of a tampering, the claimed

invention would still not have been obtained. By this measure, one of ordinary skill in the art does not arrive at the subject matter of the present application according to which "said volatile memory will be cleared upon an interruption of the received of the supply power from the terminal".

Again, the claimed invention would not have been obtained, if for some reason, one of ordinary skill in the art would think of a module having programs stored in a volatile memory, and including a power supply for powering the volatile memory and a tamper switch disconnecting the power supply from the volatile memory in case of tampering. Further, if changes in the module system take place, supplemental operating programs would be stored into this volatile memory (compare column 5, second paragraph). However, again, one of ordinary skill in the art would not have obtained the claimed subject matter of the present application.

To summarize the above, even a combination of the above documents does not arrive at the subject matter of the present application since none of these documents teaches or suggests that it would be favorable to store an algorithm code of a secure module into a volatile memory of the secure module with the module being powered by the terminal so that the algorithm code (or parts thereof) are only available for unauthorized third parties during terminal sessions. Even the embodiment of Takahira concerning the testing of the IC cards is not a basis for this idea since the tests envisaged by Takahira are only performed one time during the lifetime of the IC cards, namely before the

issuance of the IC cards. The program update embodiment described by Takahira merely addresses rarely occurring changes in the IC card system and according to this embodiment the updated program is stored in a non-volatile manner (See Column 5, lines 17-18).

It is accordingly believed to be clear that none of the references, whether taken alone or in any combination, either show or suggest the features of claims 1, 11, 13, 14, 15, or 17. Claims 1, 11, 13, 14, 15, and 17 are, therefore, believed to be patentable over the art. The dependent claims are believed to be patentable as well because they all are ultimately dependent on claim 1, 11, or 15.

In view of the foregoing, reconsideration and allowance of claims 1-17 are solicited.

In the event the Examiner should still find any of the claims to be unpatentable, counsel would appreciate receiving a telephone call so that, if possible, patentable language can be worked out.

Please charge any fees that might be due with respect to Sections 1.16 and 1.17 to the Deposit Account of Lerner Greenberg Stemer LLP, No. 12-1099.

Respectfully submitted,

/Laurence A. Greenberg/
Laurence A. Greenberg
(Reg. No. 29,308)

MPW:cgm

January 15, 2008

Lerner Greenberg Stemer LLP
P.O. Box 2480
Hollywood, Florida 33022-2480
Tel.: (954) 925-1100
Fax: (954) 925-1101